

Cybersecurity Governance

Cybersecurity governance is a framework that defines the principles, policies, and procedures for protecting information assets from cyber-attacks.



compliance**risk**
keeping your **risk** in check™

What is Cybersecurity Governance?

Definition

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

The Why -#shiftLeft

By taking a proactive approach to your cyber program, you can put in place policies, procedures, and guardrails in left of boom, before an attack occurs. This will enable you to get on the offense and be better prepared to detect, prevent, and respond to potential security incidents.

Examples

Examples of cybersecurity governance initiatives include processes for

Authorizing officials to approve policies;

End user training and adoption for employees

Create a review cadence to ensure policies are updated and maintained



NIST Cybersecurity Framework: Governance

ID.GV: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

This includes defining the roles and responsibilities of personnel, establishing policies and procedures, and managing risk. The governance framework should be designed to enable the organization to manage cybersecurity risks in a way that aligns with its overall risk management strategy.

Why is Cybersecurity Governance important?



Components for a Cybersecurity Governance program



Plan

Develop and implement a comprehensive plan for protecting information assets that takes into account the organization's unique needs and risks.



Training

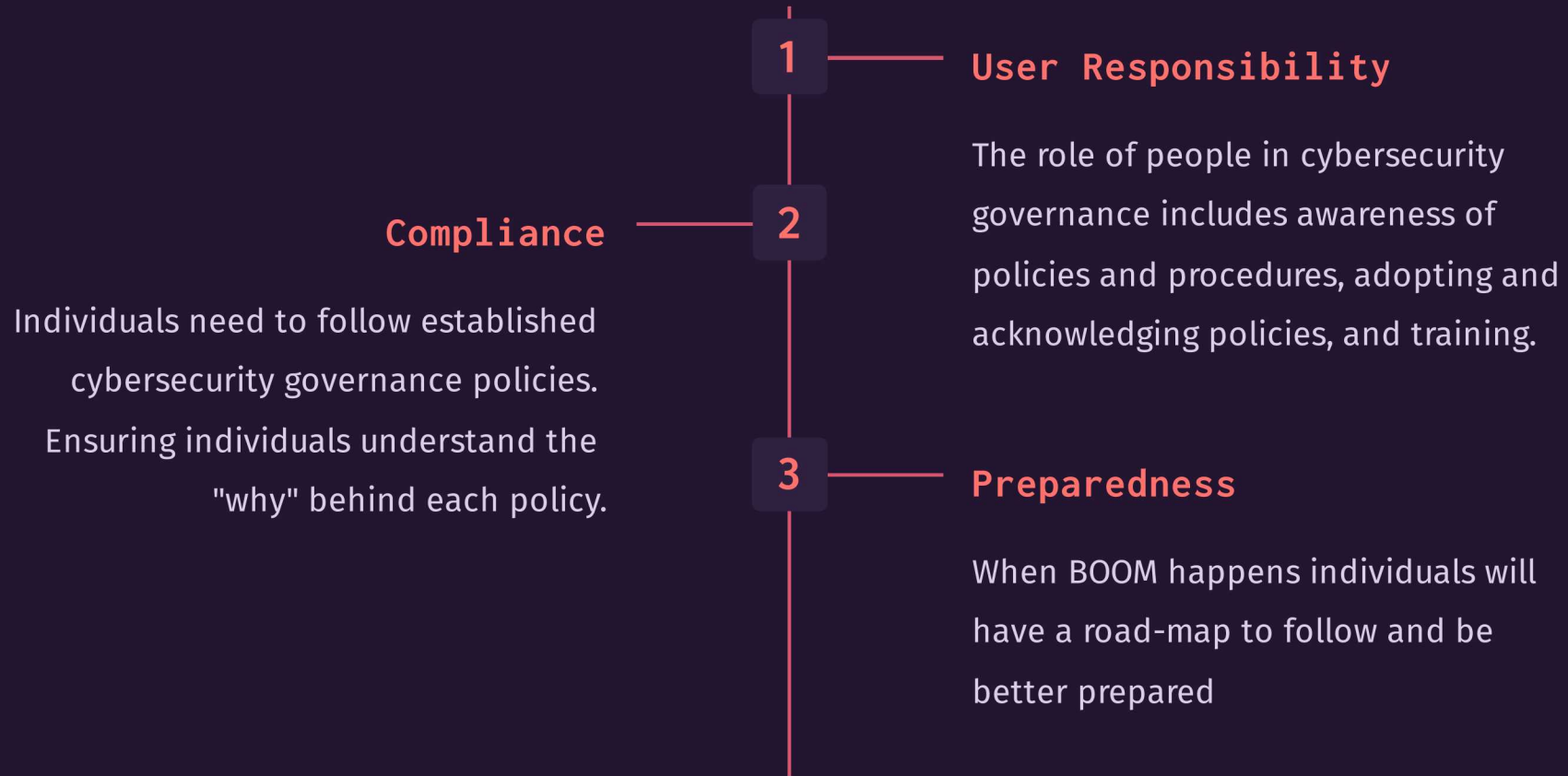
Train employees and contractors thoroughly and regularly provide awareness training to help identify and prevent security incidents caused by human errors.



Policy

Create a set of policies and procedures for information security and cybersecurity governance that should be revised annually.

The role of people in Cybersecurity Governance



The significance of processes in Cybersecurity Governance

Risk Management

A critical component of cybersecurity governance that involves identifying, assessing, and prioritizing risks associated with an organization's information assets.

Compliance and Regulations

Compliance with cybersecurity regulations and standards is another critical component of cybersecurity governance. Organizations must comply with various regulations such to ensure the protection of sensitive information.

Incident Response

Incident response planning involves preparing for and responding to cybersecurity incidents. Effective incident response planning is crucial to minimizing the impact of a cybersecurity incident and returning operations to normal as quickly as possible.

The impact of policy in Cybersecurity Governance



Coverage

Policies define what actions, behaviors, and processes are allowed or disallowed in terms of cybersecurity governance. Policies should be regularly updated to cover emerging risks and evolving threats.



Enforcement

Policies need to be enforced, monitored, and measured regularly, ensuring that employees comply with the security policies and procedures, with little room for deviation.



Response

Policies should include a standard process for handling security violations and unauthorized access, including disciplinary measures. Clear policies ensure an appropriate and timely response to a security breach.

Conclusion

1 The need for Cybersecurity Governance

The benefits of Policy Governance for CEOs and executive leaders include greater autonomy and authority, clearer expectations for performance, and a focus on strategic leadership.

2 Actionable Strategies

People, processes, and policies in cybersecurity governance can significantly reduce the risk of a cyber-attack and improve the response to such threats.

3 Best Practices

It's recommended that companies; plan, train, create policies, establish processes, and monitor compliance regularly to keep up with the ever-increasing cyber threat landscape and changing regulations.